UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/887,599	06/22/2001	Peter Yianilos	500578.2001	7240

7590 01/31/2006

STEPHEN M. CHINN
REED SNITH LLP
599 LEXINGTON AVENUE
29TH FLOOR
NEW YORK, NY 10022

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 01/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/887,599	YIANILOS ET AL.	
	Examiner	Art Unit	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 19 December 2005 have been fully considered but they are not persuasive. Applicant's argument that the specification provides support for the amendments to claims 12 and 17 that require "...that said operating system is approved to be loaded on that specific computer platform alone" is not persuasive because the description of encryption/decryption keys unique to a particular computer platform (specification page 9, lines 8-11) does not specify the use of these keys on an operating system so that the operating system can be loaded on only a specific computer platform. Similarly the specification page 6, lines 20-22 and page 8, lines 16-20, discuss verification of an operating system whereas "...verification prevents potential circumvention of the security features that are implemented by the O/S" (page 6, lines 15-17) and authenticating digital signatures respectively. Neither cited portion of the specification provides a teaching of using digital signatures, encryption/decryption keys, or any other verification or authentication methods so as to limit the loading of an operating system to one particular computer platform. Cited pages 12, line 16 through page 13, line 2, discuss merely the process by which a signature key is authenticated if it has been signed by a manufacturer. This cited portion of the specification does not disclose limiting the loading of an operating system to one particular computer platform. This portion of the specification with respect to OS verification deals with ensuring that the OS comes from a particular manufacturer and has nothing to do with the loading of the OS on any particular computer platform.

2. Applicant's argument that England does not disclose ensuring that said operating system is approved to be loaded on that specific computer platform is not persuasive because the

authentication step of England is occurring when the operating system is already installed within a computer platform. So that when the operating system is authenticated before loading, the only computer platform that the operating system can be loaded on would be the very one that it is installed on. Therefore, England meets the claim limitations because the operating system of England cannot be loaded onto another computer platform. This rationale also applies to Applicant's argument with respect to claim 17.

3. Applicant's argument that England does not disclose that the receiving platforms have a public signature identification key to authenticate said signatures is not persuasive because the applications and modules have public keys and public key signatures that are authenticatable by the receiving computer system (Col. 8, lines 57-60 & Col. 9, lines 17-20).

4. Applicant's argument that England does not disclose a plurality of hander programs because there is only a singular security manager is not persuasive because that particular security manager is on the client side and not the distributor side. England discloses that the content distributor assigns modules for handling specific content (Col. 8, lines 35-39).

5. Applicant's argument that England does not disclose a plurality of secret key encoded signature, each distinctive to a subset of application programs and object files is not persuasive because England discloses that the content distributor digitally signs each particular application so that it can be authenticated (Col. 8, line 64 – Col. 9, line 7). This rationale also applies to Applicant's arguments with respect to claim 16.

6. Applicant's argument that England fails to disclose that handler programs are programmable to permit multi-parameter control over access to the associated one of said object

files is not persuasive because Figure 4 of England shows that the modules assigned for handling the content of DLLs, which by their very nature are programmed to control access over code.

7. Applicant's argument that England does not disclose secret keys is not persuasive because secret keys are disclosed in England within the security manager, which is in the client computer (Col. 10, lines 17-19 & Figure 4). The application of a cryptographic key to data is the standard method/algorithm for creating a digital signature, and therefore the limitation is meet inherently by the teaching of creating a digital signature. This rationale also applies to Applicant's argument with respect to claim 15.

8. Applicant's argument that England does not disclose decrypting content using secret keys is not persuasive because in addition to the cited teachings, claim 18 of England shows that the security manager decrypts the content and as stated above, the security manager stores secret keys for decryption (Col. 10, lines 17-19 & Figure 4).

9. In response to applicant's argument that an Application Builder in Rose performs decryption instead of an operating system as in England, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

10. Applicant's argument that England does not disclose authenticating an operating system using digital signatures is not persuasive because England discloses (Col. 2, lines 16-40) that the operating system in question is authenticated using methods incorporated by reference. One of

those references incorporated by reference is Patent No. 6,327,652, which discloses that the operating system is verified using digital signatures (Abstract). Therefore, because the teachings of the '652 patent are incorporated by reference into the previously cited England reference, the claimed limitation is meet.

11. Applicant's argument that England does not disclose a sending station capable of creating a digital signature with a secret signature key, said secret signature key being distinctively associated with said sending station is not persuasive because England discloses that the content distributor digitally signs each particular application so that it can be authenticated (Col. 8, line 64 – Col. 9, line 7). To create a digital signature a key is need, this key meets the limitation of a secret signature key.

12. Applicant's argument that England does not disclose encrypting data with an encryption key unique to the platform is not persuasive because England discloses the system further provides for secure encrypted sessions wherein encrypted content is transmitted (Col. 11, line 55 – Col. 12, line 5). England does not disclose using keys unique to a specific computer platform. Rose discloses using cryptographic keys unique to a computer platform (Col. 10, lines 43-53). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a public key cryptography system in England wherein data is decrypted using terminal unique keys in order to verify user's as taught in Rose (Col. 10, lines 26-29). The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642

F.2d 413, 208 USPQ 871 (CCPA 1981). This rationale also applies to Applicant's argument with respect to claim 13.

13. Applicant's argument that England never discloses a decryption key that is associated with a public encryption key is not persuasive because public key encryption systems have a public and private key pair that are associated with each other. The public key acts as the encryption key and the private key acts as the decryption key. Therefore, the claim limitation is inherently meet by the public key cryptography teaching.

14. Applicant's argument that England does not disclose a hash digest is not persuasive because the result of a hash function is a digest. Therefore, the teaching of a digest inherently incorporates a hashing function.

Claim Rejections - 35 USC § 112

15. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

16. Claims 12, 17 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The added material which is not supported by the original disclosure is as follows: The operating system is approved to be loaded on that specific computer platform alone.

Claim Rejections - 35 USC § 102

17. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

18. Claims 12, 14, 16 are rejected under 35 U.S.C. 102(e) as being anticipated by England, U.S. Patent No. 6,775,779. Referring to claim 12, England discloses a computer system for content protection wherein the operating system is authenticated during the boot process before it is loaded (Col. 2, lines 16-40), which meets the limitations of a receiving platforms, each of said receiving platforms having firmware and an operating system, said firmware authenticating said operating system. The fact that the operating system is authenticated on the computer system meets the limitation of the operating system being approved to be loaded on that specific computer platform alone. The system uses a "secure pages" architecture that is capable of running designated processes, libraries, or other software components (Col. 2, lines 65-67), which meets the limitation of said hardware having memory in which application programs and object files can be stored. This "secure pages" architecture runs the programs at a higher level of protection. For example, rights management operating system modules, communications drivers, and video decoding applications programs can run in protected memory that is not accessible by other OS modules and device drivers and by other applications outside the OS (Col. 3, lines 1-9), which meets the limitations of said operating system capable of creating a firewall around data in memory pertaining to application programs and object files to control access to said application programs and object files, and said firewall around said data in memory being capable of

allowing said application programs to access said data in memory when approval of access is obtained from said application program and from said data in memory because Applicant defines the "firewall" as an arrangement in the computer platform that performs memory management in the form of access control. The system can decrypt and authentication encrypted content that is provided to the system (Col. 8, line 64 – Col. 9, line 29), which meets the limitation of a plurality of a sending station, each of said receiving platforms being adapted to receive said application programs, object files, handlers and signatures, an input interface connected to said platform to allow input data to be received by said platform and said operating system capable of decrypting said input data and of authenticating said input data. The system further provides for secure encrypted sessions wherein encrypted content is transmitted (Col. 11, line 55 – Col. 12, line 5), which meets the limitation of an output interface connected to said platform to allow said platform to transmit output data out of said platform, and said output data being encrypted when transmitted. England discloses that the digital signature is created with a public key (Col. 9, lines 18-20), which meets the limitation of operating system authenticates said input data by verifying a digital signature associated with said input data with a public signature key and input data that is not authenticated by said operating system is classified as insecure data.

Referring to claim 14, England discloses that the digital signature is created with a secret key (Col. 11, lines 6-17).

Referring to claim 16, England discloses that the digital signature is created with a public key (Col. 9, lines 18-20), which meets the limitation of each receiving platform having a plurality of public signature identification keys to correspond to the plurality of secret keys at said sending station.

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

21. Claims 1, 2, 4-11, 13, 15, 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over England, U.S. Patent No. 6,775,779, in view of Rose, U.S. Patent No. 5,708,709. Referring to claims 1, 8, 9, 13, 17, 19, 20, England discloses a computer system for content protection wherein the operating system is authenticated during the boot process before it is loaded (Col. 2, lines 16-40), which meets the limitations of a computer platform having hardware capable of authenticating an operating system to be loaded on said hardware and preventing said operating system from being loaded onto said hardware when said operating system is not authenticated. The fact that the operating system is authenticated on the computer system meets the limitation of the operating system being approved to be loaded on that specific computer platform alone. The system uses a "secure pages" architecture that is capable of running designated processes, libraries, or other software components (Col. 2, lines 65-67),

which meets the limitation of said hardware having memory in which application programs and object files can be stored. This "secure pages" architecture runs the programs at a higher level of protection. For example, rights management operating system modules, communications drivers, and video decoding applications programs can run in protected memory that is not accessible by other OS modules and device drivers and by other applications outside the OS (Col. 3, lines 1-9), which meets the limitations of said operating system capable of creating a firewall around data in memory pertaining to application programs and object files to control access to said application programs and object files, and said firewall around said data in memory being capable of allowing said application programs to access said data in memory when approval of access is obtained from said application program and from said data in memory because Applicant defines the "firewall" as an arrangement in the computer platform that performs memory management in the form of access control. The system can decrypt and authentication encrypted content that is provided to the system (Col. 8, line 64 – Col. 9, line 29), which meets the limitation of an input interface connected to said platform to allow input data to be received by said platform and said operating system capable of decrypting said input data and of authenticating said input data. The system further provides for secure encrypted sessions wherein encrypted content is transmitted (Col. 11, line 55 – Col. 12, line 5), which meets the limitation of an output interface connected to said platform to allow said platform to transmit output data out of said platform, and said output data being encrypted when transmitted. England discloses that the content is decrypted using secret keys (Col. 11, lines 6-30), but does not disclose that the decryption key is a private decryption key unique to a specific computer platform. Rose discloses a method for try and buy application programs wherein a the programs are encrypted and transmitted to users who decrypt

them with private keys that are unique to their user terminals (Col. 10, lines 43-53), which meets the limitation of said operating system decrypts said input data with a private decryption key unique to that specific computer platform to ensure that said input data is authorized for access on said specific computer platform alone. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a public key cryptography system in England wherein data is decrypted using terminal unique private keys in order to verify the user's rights to execute the trial application program as taught in Rose (Col. 10, lines 26-29).

Referring to claims 2, 18, England discloses that the operating system authentication uses digital signatures for verification (Col. 2, lines 16-40).

Referring to claim 4, England discloses that the digital signature is created with a public key (Col. 9, lines 18-20), which meets the limitation of operating system authenticates said input data by verifying a digital signature associated with said input data with a public signature key and input data that is not authenticated by said operating system is classified as insecure data.

Referring to claims 5, 10, England discloses that public keys are used for data encryption (Col. 9, lines 43-55).

Referring to claim 6, England discloses that the digital signature is created with a secret key (Col. 11, lines 6-17).

Referring to claim 7, England discloses a secure handler located in secure memory that controls access to the secure memory (Col. 7, lines 37-49), which meets the limitation of data in memory gives approval for access through an object handler associated with each of said object files when said data in memory pertains to said object files.

Referring to claim 11, England discloses that the authentication procedure can be performed by a hash digest (Col. 9, lines 43-45).

Referring to claim 15, England discloses that the digital signature is created with a secret key (Col. 11, lines 6-17).

Conclusion

22. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100